p-adic number.

8. The method of claim 1 in which said first and second parts analyze a sequence of elliptic curves.

9. The method of claim 8 in which said analysis generates a cryptographic key for use in a digital processing system.

ABSTRACT OF THE DISCLOSURE

[44] The present invention comprises fast new methods for computing high-precision solutions of Frobenius equations that arise in elliptic-curve cryptography. In particular, this invention may be used to accelerate the computation of the number of points on an elliptic curve over a finite field. The advantage over methods in prior art is that the invention is faster than previously known methods. The methods enable optimally fast canonical lifting of elliptic curves defined over finite fields, optimally fast pre-computations to determine an efficient representation of intermediate quantities, and optimally fast lifting of finite-field elements to compute multiplicative representatives. Furthermore the invention enables rapid computation of norms and traces amongst other applications.

DRAWINGS

[45] The drawings are illustrated in figures 1 and 2.

OATH OR DECLARATION

[46] The oath or declaration is attached on form PTO / SB / 01A, "Declaration for Utility or Design Application Using An Application Data Sheet".

SEQUENCE LISTING

[47] Not Applicable.